Gouvernement du Canada | Government of Canada

DEUXIÈME RAPPORT D'ÉTAPE SUR LES

ÉVOLUTIONS EN MATIÈRE DE LÉGISLATION SUR LA PROTECTION DES DONNÉES AU CANADA

Rapport à la Commission européenne novembre 2017

Canada

Cette publication est également offerte en ligne http://www.ic.gc.ca/eic/site/113.nsf/fra/h_07661.html.

Pour obtenir un exemplaire de cette publication ou un format substitut (Braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication : www.ic.gc.ca/demande-publication ou communiquer avec:

Centre de services Web
Innovation, Sciences et Développement économique Canada
Édifice C.D. Howe
235, rue Queen
Ottawa (Ontario) K1A 0H5
Canada

Téléphone (sans frais au Canada) : 1-800-328-6189
Téléphone (international) : 613-954-5031
TTY (pour les personnes malentendantes) : 1-866-694-8389
Les heures de bureau sont de 8 h 30 à 17 h (heure de l'Est)
Courriel : ISDE@Canada.ca

Autorisation de reproduction

À moins d'indication contraire, l'information contenue dans cette publication peut être reproduite, en tout ou en partie et par quelque moyen que ce soit, sans frais et sans autre permission du ministère de l'Industrie, pourvu qu'une diligence raisonnable soit exercée afin d'assurer l'exactitude de l'information reproduite, que le ministère de l'Industrie soit mentionné comme organisme source et que la reproduction ne soit présentée ni comme une version officielle ni comme une copie ayant été faite en collaboration avec le ministère de l'Industrie ou avec son consentement.

Pour obtenir l'autorisation de reproduire l'information contenue dans cette publication à des fins commerciales, veuillez demander l'affranchissement du droit d'auteur de la Couronne : www.ic.gc.ca/demande-droitdauteur ou communiquer avec le Centre de services Web aux coordonnées ci-dessus.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de l'Industrie, (2018).

N° de catalogue lu37-8/2-2018F-PDF
ISBN 978-0-660-27310-5

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

Also available in English under the title *Second Update Report on Developments in Data Protection Law in Canada*.

Table des matières

1.0 Contexte 4

2.0 Évolutions des lois fédérales du Canada sur la protection des renseignements personnels 4

3.0 Précisions au sujet du rapport d'étape de mai 2017 8

4.0 Renseignements supplémentaires et rapports 19

1.0 Contexte

1.1 En décembre 2001, la Commission européenne (CE) rendait la Décision 2002/2/CE, conformément au paragraphe 6 de l'article 25 de la Directive 95/46/CE. Cette décision précise que le Canada est considéré comme assurant un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne (UE) aux destinataires assujettis à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

1.2 Conformément à l'article 2 de la Décision d'exécution (UE) 2016/2295, la CE est maintenant tenue de suivre, de manière permanente, les évolutions de l'ordre juridique canadien, y compris celles touchant l'accès des autorités publiques aux données à caractère personnel, afin d'évaluer si le Canada continue d'assurer un niveau de protection adéquat des données à caractère personnel.

1.3 En mai 2017, dans le cadre d'un effort continu visant à aider la Commission à s'acquitter de son obligation de surveillance, les représentants du gouvernement du Canada ont remis aux représentants de la CE le premier de plusieurs rapports périodiques décrivant les évolutions du cadre de protection des données du Canada applicable aux organisations du secteur privé et aux entités gouvernementales depuis la Décision 2002/2/CE, ainsi que des renseignements sur les limitations et les mesures de protection régissant l'accès des autorités publiques aux données à caractère personnel. D'autres consultations ont eu lieu entre les représentants du Canada et de la CE dans le cadre d'une vidéoconférence de suivi en juillet 2017.

1.4 Le 25 septembre 2017, Innovation, Sciences et Développement économique Canada a fourni à la Commission européenne des renseignements supplémentaires, sous forme d'addenda au premier rapport d'étape, à titre de suivi de la discussion par vidéoconférence, au cours de laquelle les représentants de la CE ont demandé des précisions sur plusieurs éléments du rapport sur les évolutions. L'addenda fournit de plus amples renseignements sur le rôle et les responsabilités du Commissariat à la protection de la vie privée du Canada en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

1.5 Le présent rapport :

- clarifie davantage les questions en suspens sur le cadre canadien soulevées par les représentants de la CE lors de la vidéoconférence du 13 juillet;
- décrit les évolutions du cadre de protection des données du Canada intervenues depuis le premier rapport d'étape, préparé en mai 2017.

2.0 Évolutions des lois fédérales du Canada sur la protection des renseignements personnels

Règlement concernant les atteintes à la protection des données en vertu de la LPRPDE

2.1 En 2015, la loi canadienne régissant la protection des renseignements personnels dans le secteur privé, la *Loi sur la protection des renseignements personnels et les documents électroniques*, a été modifiée afin d'obliger les organisations à signaler les atteintes graves aux mesures de sécurité des données. Ces dispositions entreront en vigueur une fois le règlement prêt, lequel précisera davantage les exigences législatives, comme les exigences minimales pour la présentation de rapports sur les atteintes à la sécurité des données au commissaire à la protection de la vie privée, la

notification aux personnes touchées ainsi que la portée et la période de conservation des dossiers sur les atteintes à la protection des données.

2.2 Une ébauche du *Règlement concernant les atteintes aux mesures de sécurité* a été publiée le 2 septembre 2017 dans la Partie I de la *Gazette du Canada*. Le projet de règlement se trouve sur le site Web de la *Gazette du Canada* (voir http://gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-fra.html).

2.3 Innovation, Sciences et Développement économique Canada a sollicité les commentaires et les opinions des parties intéressées sur le projet de règlement jusqu'au 2 octobre 2017. Les commentaires reçus aident à formuler le règlement final, qui devrait être publié dans la Partie II de la *Gazette du Canada* au cours du premier semestre de 2018.

Étude de la LPRPDE par un comité parlementaire

2.4 Le 14 février 2017, un comité de la Chambre des communes a entrepris une étude de la LPRPDE dans le cadre d'une série d'examens législatifs portant sur la protection de la vie privée au Canada. Dans le cadre de ses travaux, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique a entendu 65 témoins représentant le secteur privé, la société civile, le milieu universitaire, le Commissariat à la protection de la vie privée du Canada et d'autres autorités nationales et internationales chargées de la protection des données. Le Comité a sollicité les points de vue et les opinions de témoins sur des questions clés, qu'il fallait, selon le commissaire à la protection de la vie privée du Canada, examiner plus à fond, à savoir le régime d'application de la LPRPDE, le modèle de consentement, le concept du droit à l'oubli, la nécessité de règles spéciales pour les enfants en ligne et, enfin, l'importance de conserver le statut d'adéquation de l'UE. Bien que l'étude de la LPRPDE ne soit pas considérée comme un examen législatif officiel de la Loi, le Comité a entrepris un examen exhaustif dans ces domaines et devrait publier sous peu un rapport des constatations et recommandations auxquelles il en est arrivé.

Loi canadienne antipourriel (LCAP)

2.5 La Loi canadienne antipourriel (LCAP) prévoit un droit privé d'action. En vertu de ces dispositions, des particuliers et des organisations auraient pu intenter des poursuites contre des particuliers et des organisations qui, selon eux, auraient violé la loi. Les dispositions de la LCAP devaient entrer en vigueur en juillet 2017, le jour même où le Parlement devait examiner la LCAP (conformément à la Loi). Afin que les nombreux intervenants qui affirment trouver difficile d'interpréter plusieurs dispositions de la Loi tout en étant exposés au risque de litige puissent le faire en toute certitude juridique et reconnaissant qu'il est difficile pour le Parlement d'examiner les dispositions législatives dans l'abstrait, la date d'entrée en vigueur des dispositions a été suspendue le 2 juin 2017 en attendant la tenue d'un examen législatif de la LCAP.

2.6 Le 14 juin 2017, la Chambre des communes a chargé le Comité permanent de l'industrie, des sciences et de la technologie (INDU) de faire l'examen parlementaire de la LCAP. Le Comité INDU a tenu sa première réunion à ce sujet le 26 septembre 2017.

Consultations sur la sécurité nationale

2.7 Le 19 mai 2017, le Canada a publié un rapport résumant ce que nous avons appris des consultations publiques sur le cadre de sécurité nationale afin de donner aux Canadiens un aperçu des commentaires reçus au cours des consultations. Au total, environ 58 000 réponses et 17 000 courriels ont été reçus dans le cadre de ces consultations. Les

renseignements recueillis au cours de ces consultations servent à guider la prise de décisions quant aux modifications à apporter au cadre de sécurité nationale du Canada. Plus récemment, ils ont été utilisés pour élaborer le projet de loi C-59, *Loi de 2017 sur la sécurité nationale*, qui est actuellement à l'étude au Parlement du Canada et qui vise un large éventail de mesures visant à renforcer la responsabilité et la transparence, à respecter les engagements pris à l'égard de l'ancien projet de loi C-51 ainsi qu'à renforcer la sécurité et à protéger les droits.

Projet de loi – Projet de loi C-59, Loi de 2017 sur la sécurité nationale

2.8 Le gouvernement du Canada a récemment présenté un projet de loi qui renforce la surveillance des organismes de sécurité nationale par le gouvernement et propose des modifications à la *Loi sur le Service canadien du renseignement de sécurité* (SCRS). Reconnaissant que ce projet de loi fait toujours l'objet d'un débat et d'un examen au Parlement du Canada, voici une brève description des mécanismes d'examen proposés.

2.9 Office de surveillance des activités en matière de sécurité nationale et de renseignement – Le projet d'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSASNR) permettrait d'effectuer un examen complet et intégré de toutes les activités de sécurité nationale et de renseignement à l'échelle du gouvernement du Canada.

2.10 L'OSASNR remplacerait le Comité de surveillance des activités de renseignement de sécurité (CSARS) et le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) (l'organisme d'examen responsable du Centre de la sécurité des télécommunications du Canada) en plus d'assumer la responsabilité de l'examen des activités de sécurité nationale de la GRC actuellement menées par la Commission civile d'examen et de traitement des plaintes (CCETP). Il effectuerait également des examens dans les ministères et les organismes participant à des activités de sécurité et de renseignement.

2.11 L'OSASNR veillerait à ce que les organismes de sécurité nationale du Canada respectent les lois et à ce que leurs actions soient raisonnables et nécessaires. Il aurait le plein pouvoir indépendant de déterminer les activités du gouvernement à examiner. Cela comprendrait l'examen des activités en cours. Tout comme le CSARS, il jouirait également d'un accès sans restriction à tous les documents (sauf aux documents confidentiels du Cabinet).

2.12 L'OSASNR communiquerait ses constatations et recommandations aux ministres compétents dans des rapports classifiés. Il produirait également un rapport annuel non classifié à l'intention du Parlement résumant les constatations et les recommandations présentées aux ministres.

2.13 Cette nouvelle entité compléterait le travail important du Comité des parlementaires sur la sécurité nationale et le renseignement, créé récemment par le projet de loi C-22. Celui-ci ayant reçu la sanction royale, le Comité sera établi dans les mois à venir et sera chargé d'examiner le SCRS de même que d'autres ministères et organismes fédéraux. Ensemble, ils assureraient une surveillance complète des activités de sécurité nationale et de renseignement du Canada.

2.14 Commissaire au renseignement – Le gouvernement du Canada propose de créer un commissaire au renseignement (CI), un nouvel organisme de surveillance ayant un statut quasi judiciaire. Le CI aurait le mandat d'examiner certaines autorisations accordées en vertu de la *Loi sur le SCRS* et de la *Loi sur le Centre de la sécurité des télécommunications*, autorisations qui sont proposées dans le projet de loi C-59. Le CI examinerait les conclusions sur la

base desquelles les autorisations sont données et serait responsable de leur approbation si elles sont jugées raisonnables.

Décisions récentes des tribunaux

2.15 *Douez c. Facebook* – Le 23 juin 2017, la Cour suprême du Canada a rendu sa décision dans Douez c. Facebook sur l'applicabilité des clauses d'élection de for dans les contrats en ligne. M^me^ Douez a cherché à intenter des poursuites contre Facebook en Colombie-Britannique pour atteinte présumée à son droit à la vie privée. Facebook soutenait ne pas pouvoir présenter sa cause en Colombie-Britannique du fait qu'en créant son compte, M^me^ Douez avait accepté ses conditions de service, qui comprennent une clause d'élection de for précisant que les utilisateurs doivent régler toute réclamation contre l'entreprise devant un tribunal situé en Californie.

Dans sa décision, la Cour suprême du Canada a modifié le critère de common law utilisé pour déterminer si un tribunal devrait écarter une clause d'élection de for, critère qu'elle avait établi dans l'affaire Pompey. Dans cette décision, la Cour a reconnu que, bien que les facteurs énoncés dans l'arrêt Pompey aient été interprétés et appliqués de façon restrictive dans le contexte commercial, le contexte du consommateur exige la modification de ces facteurs. La majorité de la Cour suprême du Canada a reconnu que l'applicabilité de la clause d'élection de for peut différer selon le contexte contractuel. Les juges majoritaires ont donc décidé que les tribunaux devraient tenir compte des considérations de politique publique relatives à l'inégalité flagrante du pouvoir de négociation entre les parties et à la nature des droits en jeu lorsqu'ils examinent la possibilité d'appliquer une clause d'élection de for dans un contrat de consommation. La Cour suprême du Canada était d'avis que les préoccupations de politique publique relatives à l'accès aux tribunaux nationaux sont particulièrement importantes dans cette affaire étant donné qu'il s'agit d'un droit fondamental en matière de protection de la vie privée.

2.16 *Google Inc. c. Equustek Solutions* – Dans *Google Inc. c. Equustek Solutions Inc.*, la Cour suprême du Canada s'est penchée sur trois grandes questions :

i. Dans quels cas un tribunal peut-il ordonner à un moteur de recherche de bloquer certains résultats en tenant compte de l'intérêt lié à l'accès à l'information et de la liberté d'expression, et quelles limites (géographiques ou temporelles) doivent être imposées à l'égard de telles ordonnances?
ii. Les tribunaux canadiens ont-ils le pouvoir de bloquer des résultats de recherche à l'extérieur des frontières canadiennes?
iii. Dans quels cas, s'il en est, une partie peut-elle obtenir une injonction interlocutoire contre un tiers à qui rien n'est reproché?

2.17 En ce qui a trait à la première question, la Cour a déterminé que l'injonction interlocutoire est nécessaire de façon à prévenir un préjudice irréparable, car il serait impossible à Datalink d'exploiter une entreprise sur Internet sans l'aide de Google. La Cour a également déterminé que l'ordonnance ne fait pas intervenir, à première vue, des valeurs liées à la liberté d'expression. Elle vise plutôt à empêcher la commission de préjudices irréparables découlant de la vente illégale de marchandises résultant de la violation par Datalink de plusieurs ordonnances judiciaires. Pour ce qui est de la deuxième question, la Cour a déterminé que les tribunaux canadiens avaient le pouvoir d'accorder une injonction mondiale parce que le problème, en l'espèce, se pose en ligne et à l'échelle mondiale. Par conséquent, sans cette portée, l'injonction interlocutoire serait incapable d'atteindre ses objectifs de préservation des droits d'Equustek

en attendant l'issue du litige. En ce qui touche la troisième question, la Cour a déterminé que le « pouvoir d'accorder des injonctions est présumé illimité, et les injonctions destinées à maintenir l'ordre n'ont pas nécessairement à viser uniquement les parties au litige ».

2.18 *R. c. Orlandis-Habsburgo* – Dans *R. c. Orlandis-Habsburgo*, la Cour d'appel de l'Ontario a réexaminé les décisions de la Cour suprême du Canada dans *R. c. Spencer*, *R. c. Gomboc et R. c. Plant*. L'affaire concernait le partage régulier des données sur la consommation d'énergie entre un fournisseur d'électricité et la police. La Cour a conclu que, contrairement à une situation où une entreprise a communiqué des données précises à la police, craignant au vu de celles-ci qu'un crime ait été commis, la nature informelle de l'entente de partage d'information conclue entre Horizon et la police ne respectait pas la LPRPDE.

2.19 Dans ce cas-ci, la police et Horizon entretenaient une relation continue de partage des données sur les clients. Le juge Doherty a fait remarquer que, jusqu'à ce que les procédures en l'espèce commencent, Horizon n'avait jamais refusé une demande d'information de la police et a conclu que cela établissait que la police et Horizon travaillaient ensemble. Il a fait remarquer que cela était important, car cela distinguait leur situation de celle d'une entreprise ou d'un dénonciateur ayant transmis à la police des données précises, craignant au vu de celles-ci qu'un crime ait été commis. Dans sa décision, la Cour a examiné l'exception au sous-alinéa 7(3)c.1)(ii) de la LPRPDE et a conclu que l'entente informelle de partage de l'information entre le fournisseur d'énergie et la police n'était pas conforme à cette exigence. De plus, la Cour a conclu que l'exception au sous-alinéa 7(3)d)(i) de la LPRPDE, qui permet à une organisation de communiquer de sa propre initiative des renseignements personnels à une institution gouvernementale parce qu'elle a « des motifs raisonnables de croire que le renseignement est afférent à une contravention au droit fédéral », ne permet pas la communication informelle de renseignements à la police.

Rapport annuel 2017 au Parlement du Commissariat à la protection de la vie privée du Canada (CPVP)

2.20 En septembre 2017, le CPVP a publié son rapport annuel au Parlement[1]. Ce rapport couvre à la fois la *Loi sur la protection des renseignements personnels*, qui s'applique aux pratiques de traitement des renseignements personnels des ministères et organismes gouvernementaux, et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la loi fédérale sur la protection des renseignements personnels dans le secteur privé.

3.0 Précisions au sujet du rapport d'étape de mai 2017

3.1 Le présent segment du rapport comprend des renseignements supplémentaires visant à compléter le rapport d'étape de mai 2017 en réponse à diverses demandes d'éclaircissements additionnels de la CE. Les numéros de section du rapport de mai 2017 ont été inclus dans les rubriques aux fins de référence. En septembre 2017, des renseignements supplémentaires ont également été fournis séparément dans un addenda qui décrit davantage le rôle et les responsabilités qui incombent au commissaire à la protection de la vie privée du Canada en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Ces éclaircissements sont fondés sur la législation en vigueur et, par conséquent, ne reflètent pas les initiatives, les examens ou les évolutions en cours décrits à la section 2 du présent rapport.

[1] Le rapport est disponible en ligne à https://www.priv.gc.ca/media/4586/opc-ar-2016-2017_fra-final.pdf.

Exceptions au consentement dans l'intérêt public en vertu de la LPRPDE – Section 3.11

3.2 En général, la LPRPDE exige qu'une organisation obtienne le consentement d'une personne si elle recueille, utilise ou communique ses renseignements personnels à une autre organisation ou à une institution gouvernementale ou subdivision d'une institution gouvernementale. Cependant, le législateur reconnaît qu'il faut, lors de circonstances bien précises, trouver un juste équilibre entre le droit à la vie privée d'une personne et d'autres droits fondamentaux et intérêts publics. Ainsi, la Loi prévoit des exceptions à la règle générale pour permettre aux organisations de communiquer des renseignements personnels sans le consentement ou à l'insu d'une personne. Les articles de la LPRPDE relatifs à la question soulevée portent sur les exceptions législatives permettant à une organisation de communiquer des renseignements personnels d'une personne sans le consentement de celle-ci à une autre organisation ou entité gouvernementale.

3.3 Le sous-alinéa 7(3)c.1)(iv) de la Loi permet la communication de renseignements personnels par une organisation à une institution gouvernementale qui en a fait la demande dans le but de communiquer avec le plus proche parent ou le représentant autorisé d'une personne blessée, malade ou décédée, et ce, sans exiger de mandat, d'assignation ou d'ordonnance. Pour qu'une institution gouvernementale puisse se prévaloir de cette exception, elle doit satisfaire aux exigences juridiques de la Loi.

3.4 Premièrement, l'institution gouvernementale doit demander l'information et en justifier le besoin. Deuxièmement, la demande de communication doit avoir pour but explicite de communiquer avec le plus proche parent ou le représentant autorisé d'une personne blessée, malade ou décédée. Enfin, l'institution gouvernementale doit mentionner la source de l'autorité légitime étayant son droit d'obtenir l'information.

3.5 L'alinéa 7(3)d.3) de la Loi est une disposition permissive en ce sens qu'une organisation peut, de sa propre initiative, communiquer des renseignements personnels sans consentement afin de prévenir un cas d'exploitation financière ou d'enquêter sur un tel cas. La communication peut être faite à une institution gouvernementale, au plus proche parent de l'intéressé ou à son représentant autorisé. De telles communications exigent le respect de certaines conditions législatives : l'organisation a des motifs raisonnables de croire que l'intéressé a été, est ou peut être victime d'exploitation financière; la communication est faite uniquement à des fins liées à la prévention de l'exploitation ou à une enquête y ayant trait; il est raisonnable de s'attendre à ce que la communication effectuée au su ou avec le consentement de l'intéressé compromettrait la capacité de prévenir l'exploitation ou d'enquêter sur celle-ci.

3.6 Cette disposition vise à permettre aux institutions financières de prendre des mesures pour prévenir l'exploitation financière des personnes âgées et d'autres clients vulnérables, y compris, par exemple, les cas d'utilisation non autorisée de cartes de crédit et de débit, les désignations contradictoires de procuration ou l'abus de procuration, et les comptes bancaires conjoints susceptibles d'abus si le titulaire du compte conjoint utilise l'argent de la personne âgée à ses propres fins.

3.7 L'alinéa 7(3)d.4) de la Loi prévoit qu'une organisation peut, sans consentement, communiquer des renseignements personnels à une institution gouvernementale, à un proche parent ou à un représentant autorisé afin d'identifier des personnes qui peuvent être malades, blessées ou décédées. Si l'intéressé est vivant, l'organisation doit l'informer de la communication, et ce, par écrit et dès que possible. L'objet sous-jacent de cet alinéa est de permettre la communication de renseignements personnels dans des situations qui rendent difficile ou impossible d'obtenir le

consentement, comme les accidents et les catastrophes, afin d'aider à identifier des personnes décédées, blessées et malades. Par exemple, en vertu de ce sous-alinéa, les dentistes pourraient fournir et communiquer les dossiers dentaires d'un patient à une autorité gouvernementale ou à un membre de la famille afin d'identifier les victimes d'une catastrophe naturelle.

Exceptions au consentement pour la communication de renseignements en vertu de la LPRPDE – Section 3.12

3.8 Les alinéas 7(3)d.1) et 7(3)d.2) de la Loi, qui portent respectivement sur les enquêtes du secteur privé et les activités de lutte contre la fraude, prévoient qu'une organisation peut, à la différence d'une institution gouvernementale, communiquer des renseignements personnels sans consentement à une autre organisation. La LPRPDE prévoit que des conditions doivent être remplies pour que l'on puisse invoquer légalement l'une ou l'autre de ces exceptions.

3.9 En ce qui concerne l'alinéa 7(3)d.1), les renseignements communiqués doivent être destinés à la tenue d'une enquête sur la violation d'un accord ou sur la contravention au droit fédéral ou provincial et il doit être raisonnable de s'attendre à ce que la communication effectuée au su et avec le consentement de l'intéressé compromettrait l'enquête. Elle doit porter sur une contravention ou une violation qui a été commise ou qui est en train ou sur le point de l'être. Les renseignements ne peuvent pas être communiqués simplement parce que l'on *pourrait* enfreindre le contrat ou violer l'accord.

3.10 À titre d'exemple, une telle disposition pourrait être invoquée dans le cas d'une enquête sur l'inconduite professionnelle d'associations professionnelles autoréglementées telles que les collèges des médecins et chirurgiens et les ordres des juristes. Un organisme de réglementation peut être tenu d'examiner les activités bancaires illicites d'un membre contre qui une allégation a été déposée, ce qui, par conséquent, l'obligerait à obtenir les renseignements bancaires d'une institution financière. L'absence de ces exceptions législatives pourrait empêcher de telles organisations de contester les allégations d'actes répréhensibles commis par leurs membres.

3.11 En ce qui concerne l'alinéa 7(3)d.2), les renseignements communiqués sans consentement doivent avoir pour but légitime de prévenir la fraude, de la détecter ou d'y mettre fin dont la commission est vraisemblable, dans un premier temps, et, dans un deuxième temps, il doit être raisonnable de s'attendre à ce que la communication effectuée au su ou avec le consentement de l'intéressé compromettrait la capacité de lutter contre la fraude. Un exemple de l'applicabilité de l'alinéa 7(3)d.2) est celui des enquêtes visant à détecter les crimes financiers ou à prévenir la fraude dans le secteur des services financiers, comme les travaux menés par le Centre de prévention du crime bancaire et le Bureau des enquêtes de l'Association des banquiers canadiens et la Division des services d'enquête du Bureau d'assurance du Canada.

Modifications corrélatives à la LPRPDE en 2004 découlant de la Loi de 2002 sur la sécurité publique – Section 3.21

3.12 En 2004, la LPRPDE a été modifiée afin de permettre la collecte et l'utilisation, par des organisations, de renseignements personnels à l'insu ou sans le consentement de l'intéressé dans le but de faire une communication à des institutions gouvernementales pour des motifs de sécurité nationale, la défense du Canada ou la conduite des affaires internationales ou lorsque la communication de ces renseignements est exigée par la loi.

3.13 En vertu du paragraphe 7(3) de la LPRPDE, les organisations étaient déjà autorisées à communiquer des renseignements personnels à l'insu de l'intéressé ou sans son consentement à des institutions gouvernementales pour des motifs de sécurité nationale, la défense du Canada et la conduite des affaires internationales ou lorsque la loi l'exigeait autrement [alinéas 7(3)c.1)i), 7(3)d)(ii) et 7(3)i) de la LPRPDE]. La modification au paragraphe 7(1) précise que les organisations peuvent également recueillir et utiliser des renseignements personnels pour faire de telles communications à des institutions gouvernementales.

3.14 La modification était nécessaire pour appuyer la *Loi sur l'aéronautique*, en vertu de laquelle les agents désignés de Transports Canada, de la Gendarmerie royale du Canada (GRC) ou du Service canadien du renseignement de sécurité (SCRS) doivent exiger qu'un transporteur aérien ou un exploitant d'un système de réservation leur fournisse les renseignements dont il dispose, ou dont il disposera dans les 30 jours, à l'égard des passagers indiqués.

Transferts d'organisations du secteur privé à des institutions gouvernementales – Section 3.21

3.15 L'alinéa 7(3)c.1) de la Loi permet la communication de renseignements personnels d'une organisation à une institution gouvernementale à l'insu de l'intéressé ou sans son consentement dans plusieurs circonstances, y compris lorsque l'institution gouvernementale soupçonne que ces renseignements sont afférents à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales.

3.16 Pour invoquer cette exception, la communication doit avoir été demandée par l'institution gouvernementale et celle-ci doit avoir mentionné la source de l'autorité légitime étayant son droit d'obtenir les renseignements et qu'elle soupçonne que ceux-ci sont afférents à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales.

3.17 Le sous-alinéa 7(3)d)(ii) permet également la communication de renseignements personnels sans le consentement d'une organisation à une institution gouvernementale pour des motifs de sécurité nationale et de défense du Canada. Cette disposition permet de faire des communications à l'initiative de l'organisation.

Pouvoirs du Commissariat à la protection de la vie privée du Canada en vertu de la Loi sur la protection des renseignements personnels – Section 4.4

3.18 La *Loi sur la protection des renseignements personnels* établit le Commissariat à la protection de la vie privée du Canada. Le Commissaire à la protection de la vie privée est un agent du Parlement dont la mission est de protéger et de promouvoir le respect de la vie privée. Le Commissaire offre des conseils et de l'information aux individus sur la façon de protéger leurs renseignements personnels. Il est également chargé d'appliquer deux lois fédérales sur la protection de la vie privée qui établissent les règles que les institutions fédérales et certaines entreprises doivent respecter lorsqu'elles traitent des renseignements personnels. Le Commissaire à la protection de la vie privée est un ombudsman indépendant qui a le pouvoir d'enquêter sur des plaintes, de formuler des recommandations concernant le respect de la *Loi sur la protection des renseignements personnels* et de présenter des rapports au Parlement. La Loi confère au Commissaire à la protection de la vie privée le droit de présenter une demande à la Cour fédérale, suite au refus d'une institution fédérale de communiquer des renseignements personnels à un individu jouissant d'un droit d'accès à ces renseignements en vertu de la Loi, après avoir obtenu le consentement de cet individu.

3.19 Les articles 4 à 8 de la *Loi sur la protection des renseignements personnels* régissent la collecte, l'usage, la communication, la conservation et le retrait des renseignements personnels par les institutions fédérales. La *Loi sur la protection des renseignements personnels* permet à toute personne, ou à son représentant, de déposer une plainte auprès du Commissaire à la protection de la vie privée pour une violation présumée des obligations prévues aux articles 4 à 8 ayant trait à des renseignements personnels la concernant[2]. Le Commissaire à la protection de la vie privée peut également prendre l'initiative d'une plainte s'il est convaincu qu'il y a des motifs raisonnables de faire enquête sur une affaire en vertu de la *Loi sur la protection des renseignements personnels*[3]. Dans le cadre d'une enquête sur toute plainte en vertu de la *Loi sur la protection des renseignements personnels*, le Commissaire à la protection de la vie privée a le pouvoir « d'assigner et de contraindre des témoins à comparaître devant lui, à déposer verbalement ou par écrit sous la foi du serment et à produire les pièces qu'il juge indispensables pour instruire et examiner à fond les plaintes dont il est saisi, de la même façon et dans la même mesure qu'une cour supérieure d'archives »[4]. Le Commissaire à la protection de la vie privée a également le pouvoir « de pénétrer dans les locaux occupés par une institution fédérale, à condition de satisfaire aux normes de sécurité établies par l'institution pour ces locaux », « de s'entretenir en privé avec toute personne se trouvant dans les locaux » et « d'examiner ou de se faire remettre des copies ou des extraits des livres ou autres documents » dans ces locaux[5].

3.20 Si le Commissaire à la protection de la vie privée conclut au bien-fondé d'une plainte, il adressera à l'institution fédérale en question un rapport présentant les conclusions de son enquête et ses recommandations. S'il le juge à propos, le Commissaire demandera à l'institution fédérale de lui donner avis, dans un délai déterminé, soit des mesures prises ou envisagées pour la mise en œuvre de ses recommandations, soit des motifs invoqués pour ne pas y donner suite[6]. Le Commissaire à la protection de la vie privée rendra également compte au plaignant des conclusions de son enquête[7]. De plus, l'article 37 de la *Loi sur la protection des renseignements personnels* confère au Commissaire à la protection de la vie privée le pouvoir précis de tenir des enquêtes en vue de contrôler l'application des articles 4 à 8 de la *Loi sur la protection des renseignements personnels* par les institutions fédérales. Si le Commissaire considère, à l'issue de son enquête, qu'une institution fédérale n'a pas appliqué les articles 4 à 8, il adressera à cette institution fédérale un rapport présentant ses conclusions ainsi que les recommandations qu'il juge indiquées[8]. L'article 37 permet au Commissaire à la protection de la vie privée d'examiner le rendement des institutions fédérales eu égard au respect des obligations prévues à la *Loi sur la protection des renseignements personnels* et par la politique gouvernementale connexe concernant la collecte, le traitement et la protection des renseignements personnels et d'en faire rapport. Cette surveillance est essentielle pour assurer la protection et la confidentialité des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels*.

3.21 S'il estime qu'une institution gouvernementale n'a pas pris les mesures correctives appropriées, le Commissaire à la protection de la vie privée peut communiquer ses conclusions dans un rapport au Parlement. Cela peut se faire dans le rapport annuel au Parlement ou, si la question est suffisamment urgente ou importante, dans un rapport spécial[9].

---

[2] Voir les alinéas 29(1)*a*) et *h*) et le paragraphe 29(2) de la *Loi sur la protection des renseignements personnels*.
[3] Voir le paragraphe 29(3) de la *Loi sur la protection des renseignements personnels*.
[4] Voir l'alinéa 34(1)*a*) de la *Loi sur la protection des renseignements personnels*.
[5] Voir les alinéas 34(1)*d*) à *f*).
[6] Voir le paragraphe 35(1) de la *Loi sur la protection des renseignements personnels*.
[7] Voir le paragraphe 35(2) de la *Loi sur la protection des renseignements personnels*.
[8] Voir le paragraphe 37(3) de la *Loi sur la protection des renseignements personnels*.
[9] Voir les articles 38 et 39 de la *Loi sur la protection des renseignements personnels*.

Mais dans la pratique, cette mesure est rarement nécessaire, car en 2016, le Commissaire à la protection de la vie privée a reconnu que « dans la grande majorité des cas, les ministères acceptent d'appliquer [ses] recommandations »[10]. Quiconque est directement touché par la décision d'une institution fédérale de recueillir, d'utiliser ou de communiquer des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels* peut contester la légalité de la décision du gouvernement au moyen d'un contrôle judiciaire en vertu de l'article 18.1 de la *Loi sur les Cours fédérales*.

Accès aux renseignements personnels – Section 4.5

3.22 La *Loi sur la protection des renseignements personnels* accorde aux citoyens canadiens, aux résidents permanents et, par extension, aux détenus et aux personnes présentes au Canada un droit d'accès à leurs renseignements personnels que possède une institution fédérale assujettie à la Loi.

3.23 La *Loi sur l'accès à l'information* (LAI) établit un droit d'accès à l'information dans les documents des institutions fédérales assujetties à la LAI[11]. Ce droit d'accès s'applique aux citoyens canadiens et aux résidents permanents et a été accordé aux personnes présentes au Canada et à toutes les sociétés présentes au Canada[12]. Un citoyen étranger qui n'est pas présent au Canada peut avoir accès à des renseignements, y compris à ses renseignements personnels, par l'entremise d'un tiers qui est présent au Canada en donnant son consentement à ce tiers.

3.24 Dans un tel scénario, le tiers présenterait une demande d'accès à une institution fédérale et la preuve du consentement du citoyen étranger à la demande de renseignements personnels pour les dossiers contenant les renseignements personnels dudit citoyen étranger. L'institution fédérale qui répond à la demande peut communiquer au demandeur tout document contenant les renseignements personnels du citoyen étranger si celui-ci y consent.

Concepts d'une « attente raisonnable en matière de respect de la vie privée » et de « motifs raisonnables de croire » – Sections 5 et 6

3.25 Comme il est mentionné à la section 5 du rapport d'étape de mai 2017, la jurisprudence en vertu *de la Charte canadienne des droits et libertés* impose certaines exigences constitutionnelles aux mesures de l'État impliquant une attente en matière de respect de la vie privée. Le concept d'« attente raisonnable en matière de respect de la vie privée » sert à déterminer si les mesures de protection prévues à l'article 8 s'appliquent à une action de l'État donnée. Comme il est mentionné à la section 6 du même rapport, le concept de « motifs raisonnables de croire » est un fardeau de la preuve défini qui sert à déterminer si les exigences relatives à l'autorisation d'une fouille ou perquisition ont été satisfaites. Comme on l'a demandé, voici une analyse plus détaillée de ces deux concepts.

3.26 Attente raisonnable en matière de respect de la vie privée – L'article 8 de la *Charte canadienne des droits et libertés* protège contre les fouilles, les perquisitions ou les saisies abusives. La Cour suprême du Canada a défini comme une « fouille » ou « perquisition » toute action de l'État impliquant une attente raisonnable en matière de respect de la vie privée[13]. Le concept d'« attente raisonnable en matière de respect de la vie privée » est donc utilisé pour déterminer

[10] Le Commissaire à la protection de la vie privée a fait cette déclaration le 10 mars 2016 devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Le texte de la déclaration du Commissaire est disponible en ligne à https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2016/parl_20160310/ (dernière consultation le 25 octobre 2017).
[11] Voir le paragraphe 4(1) de la *Loi sur l'accès à l'information* (LAI).
[12] Voir le paragraphe 4(1) de la LAI et l'article 2 du *Décret d'extension n° 1 (Loi sur l'accès à l'information)*.
[13] *Hunter et al. c. Southam Inc.*, [1984] 2 RCS 145 (« *Southam* »).

si, en tant que seuil, les protections prévues à l'article 8 sont appliquées. Le degré de cette attente de respect de la vie privée est ensuite utilisé dans l'exercice d'équilibrage visant à déterminer si une loi autorisant une fouille ou perquisition est raisonnable – c'est-à-dire si elle est justifiable à la lumière de l'objectif de l'État, compte tenu de toute garantie prévue par la loi.

3.27 Bien que le concept ait d'abord été emprunté à la jurisprudence américaine en vertu du Quatrième Amendement[14], il a depuis pris sa propre signification et fait l'objet de sa propre analyse dans la jurisprudence canadienne en vertu de la *Charte*. Contrairement aux mesures de protection prévues par la *Loi sur la protection des renseignements personnels*, l'article 8 ne régira pas *toutes* les mesures de collecte, d'utilisation ou de communication de renseignements sur une personne, mais seulement celles qui impliquent une attente raisonnable en matière de respect de la vie privée.

3.28 On détermine l'existence et la portée d'une attente raisonnable en matière de respect de la vie privée en examinant l'ensemble des circonstances entourant la mesure de l'État[15]. Quatre questions guident l'application du critère[16] :

i. l'examen de l'objet de la fouille;
ii. la question de savoir si le demandeur possédait un droit direct à l'égard de l'objet;
iii. la question de savoir si le demandeur avait une attente subjective en matière de respect de sa vie privée relativement à l'objet;
iv. la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable.

3.29 La première question, l'examen de l'objet de la fouille, vise à déterminer la nature des intérêts en matière de respect de la vie privée en jeu dans une situation donnée et à focaliser le reste de l'analyse. La Cour suprême du Canada a cerné trois grandes « catégories » du droit au respect de la vie privée susceptibles d'être visées par les mesures gouvernementales, mais également de se chevaucher. Il s'agit du droit à la vie privée qui a trait à la personne (le droit de refuser toute palpation ou exploration corporelle), du droit à la vie privée qui a trait aux lieux (l'idée que certains lieux, comme la résidence, commandent une protection plus grande de la vie privée) et du droit au respect du caractère privé des renseignements personnels (l'idée que les personnes peuvent s'attendre à ce qu'on respecte le caractère privé de certains renseignements)[17].

3.30 La deuxième question porte sur la nature de la relation de la personne avec l'objet de la fouille. Un demandeur doit démontrer qu'il y a eu atteinte à sa propre vie privée, par opposition à celle de tierces parties.

3.31 La troisième question vise à déterminer si la personne pouvait subjectivement s'attendre au respect de sa vie privée compte tenu de l'objet de la fouille. Par exemple, une personne n'aura probablement pas d'attente subjective de respect de sa vie privée dans le cas de renseignements rendus publics (par exemple un numéro de téléphone inscrit). L'existence d'une attente subjective de respect de sa vie privée n'est toutefois pas déterminante. Le respect de la vie

[14] *Katz c. États-Unis* (1967) 389 É.-U. 247.
[15] *R. c. Edwards*, [1996] 1 RCS 128, au par. 45
[16] *R. c. Cole* 2012 CSC 53.
[17] Les atteintes au caractère privé des renseignements personnels peuvent découler d'une vaste gamme de mesures, y compris certains cas d'échange de renseignements et d'interception électronique. Une « fouille », aux fins de l'article 8, ne se limite pas à une fouille physique.

privée est un concept normatif et l'analyse des attentes raisonnables de respect de la vie privée porte sur ce à quoi une personne *devrait* être en droit de s'attendre dans une société libre et démocratique[18].

3.32 La quatrième question consiste à examiner divers facteurs afin de déterminer s'il est objectivement raisonnable pour une personne de s'attendre au respect de sa vie privée dans le contexte de la situation particulière. Bien qu'il n'y ait pas de liste exhaustive des facteurs, les facteurs pertinents dans le contexte de l'accès aux données sur les clients peuvent comprendre les suivants :

- *La question de savoir si l'objet de la fouille ou perquisition était entre les mains de tiers et, le cas échéant, si ces parties avaient une obligation de confidentialité.* Par exemple, une demande à une banque pour obtenir les dossiers bancaires d'une personne comportera une attente raisonnable en matière de respect de la vie privée[19].
- *Si la méthode de « fouille » ou de « perquisition » était invasive.* Par exemple, l'interception secrète de communications en cours est considérée comme particulièrement intrusive[20].
- *La nature de l'information recueillie*, puisque l'article 8 vise à protéger un « ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État »[21]. Cela comprend des renseignements qui tendent à révéler des détails intimes sur le mode de vie et les choix personnels de la personne[22]. Par exemple, les émanations de chaleur d'un immeuble n'entraîneront pas une attente raisonnable en matière de respect de la vie privée en raison des renseignements limités qu'ils révèlent[23], tandis que les renseignements sur les abonnés associés à une adresse IP liée à une activité en ligne le feront puisqu'ils pourraient révéler des renseignements de nature délicate[24].
- Le contexte dans lequel la « fouille » ou « perquisition » a lieu. Par exemple, les inspections de conformité et les exigences en matière de documents dans une industrie fortement réglementée impliqueront des attentes plus faibles en matière de respect de la vie privée que les fouilles ou perquisitions menées à des fins criminelles et seront donc assorties de mesures de protection moins nombreuses[25].
- La nature du lien entre le motif de la collecte initiale des renseignements et le motif de leur communication subséquente. Étant donné que les personnes peuvent généralement s'attendre à ce que les renseignements confidentiels soient utilisés aux fins pour lesquelles ils ont été fournis, l'utilisation subséquente de ces renseignements à des fins non connexes peut susciter une attente raisonnable en matière de respect de la vie privée[26].

---

[18] *R. c. Tessling* 2004 CSC 67 (« *Tessling* »), au par. 42.
[19] *Del Zotto c. Canada*, [1997] 3 RCF 40 (CAF)
[20] *R. c. Tse* 2012 CSC 16 (« *Tse* »), au par. 17; *R. c. TELUS Communications Co.*, 2013 CSC 16
[21] *R. c. Plant*, [1993] 3 RCS, 281 à 293
[22] *Ibid.*
[23] *Tessling.*
[24] *R. c. Spencer* 2014 CSC 43.
[25] *British Columbia Securities Commission c. Branch*, [1995] 2 SCR 3
[26] *R. c. Dyment*, [1988] 2 RCS 417, au par. 30-31

3.33 *Motifs raisonnables de croire* – Les « motifs raisonnables de croire » sont la norme d'usage courant dans les lois fédérales régissant la préautorisation judiciaire des fouilles ou perquisitions au Canada[27]. Cette norme est interchangeable avec celle des « motifs raisonnables et probables » et équivaut au libellé de la « cause probable » figurant dans la *Déclaration des droits* américaine[28]. En vertu du *Code criminel*, par exemple, pour accorder un mandat, un officier de justice doit avoir des motifs raisonnables de croire qu'une infraction a été commise et qu'il y a des preuves à trouver au lieu de perquisition[29]. En vertu de la *Loi sur le Service canadien du renseignement de sécurité*[30], l'octroi d'un mandat doit être fondé sur des motifs raisonnables de croire que l'utilisation d'une technique d'enquête particulière est nécessaire pour enquêter sur une menace à la sécurité du Canada ou pour exercer d'autres fonctions relevant du mandat du Service.

3.34 À quelques exceptions près, l'inclusion d'une disposition législative obligeant un agent à établir l'existence de motifs raisonnables de fouiller ou perquisitionner est une exigence constitutionnelle pour les lois autorisant les perquisitions dans le contexte criminel[31]. Ainsi, une loi autorisant une fouille ou perquisition qui porterait atteinte à un droit à la vie privée bien défini sans obliger l'agent à respecter la norme des « motifs raisonnables de croire » serait généralement contraire à l'article 8 de la *Charte*[32]. La norme inférieure des « motifs raisonnables de soupçonner » est utilisée pour certaines fouilles ou perquisitions qui portent atteinte à l'attente réduite en matière de respect de la vie privée, comme l'utilisation de chiens renifleurs[33].

3.35 *Application de la norme des « motifs raisonnables de croire »* – La Cour suprême du Canada a établi que la norme des motifs raisonnables de croire est une « probabilité crédible » ou une « probabilité raisonnable »[34]. Il y aura des motifs raisonnables de croire s'il existe un fondement objectif reposant sur des renseignements concluants et dignes de foi[35]. La norme est donc plus élevée que celle de la croyance raisonnable de l'existence *possible* d'éléments de preuve pertinents ou de la croyance raisonnable que des éléments de preuve *peuvent* être découverts sur les lieux au cours de la perquisition[36]. Les motifs raisonnables de croire exigent plus qu'un soupçon ou une possibilité, mais moins qu'une preuve selon la prépondérance des probabilités[37].

3.36 La Cour suprême a statué que l'application du critère des motifs raisonnables exige une évaluation subjective et objective des faits[38]. Premièrement, l'agent doit croire subjectivement que des motifs raisonnables justifient les mesures prises et, deuxièmement, il doit être établi objectivement que des motifs raisonnables existent bel et bien[39]. Autrement dit, y a-t-il suffisamment de preuves pour appuyer la croyance subjective de l'agent[40]?

---

[27] Les « motifs raisonnables de croire » servent également de norme dans plusieurs autres contextes juridiques, comme pour les décisions d'arrestation d'une personne, certaines décisions relatives à l'immigration et certaines décisions administratives et réglementaires. Il s'agit d'un fardeau de la preuve bien compris en droit canadien.

[28] *Baron c. R.*, [1993] 1 RCS 416, au par. 54, 55; *Southam*, au par. 43.

[29] *Code criminel*, L.R.C. 1985, ch. C-46, par. 487(1).

[30] *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23, al. 21(2)a).

[31] *R. c. Kang-Brown*, 2008 CSC 18, au par. 146; *Southam*, à 167-168.

[32] *Ibid.*

[33] *Ibid.*

[34] *Baron*, au par. 54; *Southam*, au par. 43.

[35] *Mugesera*, au par. 114.

[36] *Southam*, au par. 42.

[37] *Mugesera c. Canada (Ministre de la Citoyenneté et de l'Immigration)* 2005 CSC 40 (« *Mugesera* »), au par. 114. Voir également *R. c. Shepherd* 2009 CSC 35 (« *Shepherd* »), au par. 23; *R. c. Debot*, [1989] 2 RCS 1140, au par. 54.

[38] *Tse*, au par. 33; *R. c. Bernshaw*, [1995] 1 RCS 254 (« *Bernshaw* »), au par. 62; *R. c. Storrey*, [1990] 1 RCS 241 (« *Storrey* »), aux par. 16 et 17.

[39] *Tse*, au par. 33; *Bernshaw*, au par. 62; *Storrey*, aux par. 16 et 17.

[40] *Shepherd*, au par. 3.

3.37 L'ensemble des circonstances – tous les faits et les facteurs alors à la disposition de l'agent – devraient être pris en compte pour déterminer s'il y a des motifs raisonnables[41]. En appliquant la composante objective de la norme moindre des « motifs raisonnables de soupçonner », la Cour suprême a conclu que l'existence de motifs raisonnables devait être jugée en fonction des circonstances que la police connaissait ou aurait dû connaître au moment où la fouille a été effectuée et non en fonction de faits qui ont été révélés par la suite[42].

3.38 En résumé, pour satisfaire à la norme des « motifs raisonnables de croire », le tribunal de révision doit en conclure après examen de tous les faits qu'il était objectivement raisonnable pour le policier de croire subjectivement que les circonstances justifiaient la fouille[43]. Comme il en a été question dans le rapport d'étape de mai 2017, l'absence de ces motifs rend une fouille ou perquisition illégale et inconstitutionnelle et donne lieu à un recours possible en vertu de l'article 24 de la *Charte*.

Service canadien du renseignement de sécurité (SCRS) – Section 6.16

3.39 Le Service canadien du renseignement de sécurité (SCRS) est l'organisme national du renseignement de sécurité du Canada. Ses activités doivent être menées conformément à la *Loi sur le Service canadien du renseignement de sécurité* (*Loi sur le SCRS*), qui prévoit des exigences relatives à la collecte, à la conservation et à la communication de renseignements. Le SCRS doit également mener ses activités conformément à la *Charte canadienne des droits et libertés* et à la *Loi sur la protection des renseignements personnels*, entre autres lois.

3.40 Le rôle principal du SCRS est d'enquêter sur les activités soupçonnées de constituer des menaces envers la sécurité du Canada (au sens de l'article 2 de la *Loi sur le SCRS*) et de faire rapport de ces activités au gouvernement du Canada. Cette fonction est exécutée conformément aux exigences de l'article 12 de la *Loi sur le SCRS*, qui prescrit des exigences minimales pour la collecte de renseignements par le SCRS, et qui stipule ce qui suit : *« Le Service recueille, au moyen d'enquêtes ou autrement, **dans la mesure strictement nécessaire**, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard. » [gras d'accentuation ajouté]*

3.41 Le SCRS est également autorisé à mener des enquêtes dans le but de fournir des évaluations de sécurité aux ministères fédéraux et provinciaux ou des conseils aux ministres. Par exemple, le SCRS peut conseiller les ministres responsables de la *Loi sur l'immigration et la protection des réfugiés* et de la *Loi sur la citoyenneté* sur des questions touchant la sécurité du Canada afin d'aider à déterminer l'admissibilité de certaines personnes au Canada et demandes de citoyenneté[44].

3.42 Le SCRS est seulement autorisé à recueillir, à conserver ou à communiquer des renseignements conformément à la *Loi sur le SCRS*. Bien que d'autres lois, comme la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), renferment

---

[41] *Ibid.*, aux par. 21 et 23.
[42] *R. c. Chehil*, 2013 CSC 49, au par. 34, [2013] 3 RCS 220.
[43] *Shepherd*, au par. 22.
[44] L'article 15 autorise le Service à mener les enquêtes qui sont nécessaires en vue des évaluations de sécurité et des conseils, et il doit être lu conjointement avec les articles 13 et 14 de la *Loi sur le SCRS*.

des dispositions autorisant la communication de renseignements au SCRS par des tiers, elles ne modifient pas ou n'élargissent pas la capacité de collecte du SCRS, qui demeure en tout temps assujettie aux exigences de la *Loi sur le SCRS*. Dans tous les cas, le SCRS doit respecter les exigences de la *Loi sur le SCRS* avant de pouvoir recueillir l'information.

3.43 Le SCRS ne peut recueillir, analyser ou conserver de l'information à moins d'avoir au minimum des « motifs raisonnables » de soupçonner que l'activité constitue une menace pour la sécurité du Canada. Pour les activités d'enquête jugées plus intrusives, le Service doit obtenir une autorisation judiciaire préalable (art. 21 de la *Loi sur le SCRS*). Une telle demande d'autorisation judiciaire (ou de mandat) est entendue *ex parte*, ce qui signifie que le sujet de l'enquête n'est pas présent pendant l'audience. Permettre au sujet d'être présent porterait atteinte à la sécurité nationale du Canada étant donné que des techniques d'enquête délicates seraient révélées. De plus, le but pour lequel l'information a été recueillie (c.-à-d. enquêter sur les menaces à la sécurité du Canada) risquerait d'être révélé au sujet visé par l'enquête.

3.44 Plusieurs conditions doivent être remplies pour qu'un juge donne un mandat en vertu de l'article 21 de la *Loi sur le SCRS*, y compris l'existence de motifs raisonnables de croire qu'un mandat est nécessaire pour permettre au Service de faire enquête sur une menace envers la sécurité du Canada.

3.45 Le SCRS communique des renseignements conformément à l'article 19 de la *Loi sur le SCRS*, qui autorise la communication de renseignements à des fins précises, y compris dans l'exercice de ses fonctions et attributions en vertu de la Loi ou pour l'exécution ou le contrôle d'application de celle-ci. Le SCRS peut également communiquer au ministre des Affaires étrangères des renseignements pouvant servir dans le cadre d'une enquête ou d'une poursuite pour une infraction présumée lorsque ces renseignements concernent la conduite des affaires internationales du Canada, et au ministre de la Défense nationale lorsque ces renseignements concernent la défense du Canada.

Comité de surveillance des activités de renseignement de sécurité (CSARS) – Section 6.19

3.46 La *Loi sur le SCRS* comporte d'autres exigences régissant les activités du SCRS, lesquelles exigences sont liées à la responsabilité et à l'examen. Pour n'en nommer que quelques-unes, le SCRS doit obtenir l'approbation du ministre de la Sécurité publique et de la Protection civile avant de présenter une demande de mandat à la Cour fédérale. Le ministre donne des instructions sur toute question jugée appropriée. Ces instructions servent d'exigences supplémentaires sur la façon pour le Service de remplir son mandat. Le ministre approuve également la conclusion d'ententes ou de liens de coopération entre le SCRS et ses partenaires nationaux et étrangers. La *Loi sur le SCRS* prévoit un mécanisme d'examen rigoureux des activités de renseignement de sécurité par le Comité de surveillance des activités de renseignement de sécurité (CSARS).

3.47 *Comité de surveillance des activités de renseignement de sécurité (CSARS)* – Le CSARS a été créé en 1984; cet organisme d'examen externe indépendant est chargé de rendre compte au Parlement du Canada des activités du SCRS. Ses principales fonctions, telles qu'elles sont définies dans la *Loi sur le SCRS*, sont d'effectuer des examens approfondis des activités du SCRS, de mener des enquêtes sur les plaintes et de certifier le rapport annuel du directeur du SCRS au ministre. Le CSARS est entièrement indépendant du SCRS et du gouvernement. Il se compose d'au plus cinq membres qui sont nommés à temps partiel pour un mandat à durée déterminée et qui reçoivent l'appui d'un personnel à temps plein composé d'un directeur général et d'une équipe dévouée d'avocats, de chercheurs et d'autres professionnels.

Dans le cadre de ses examens, le CSARS a le pouvoir d'examiner tous les renseignements dont dispose le SCRS, à l'exception des documents confidentiels du Cabinet, et peut également rencontrer des représentants du SCRS. Le CSARS examine les activités du SCRS afin de garantir au Parlement et aux Canadiens que le SCRS a agi conformément à la loi dans l'exercice de ses fonctions.

3.48 Les examens du CSARS pour une année donnée portent sur un éventail d'activités du SCRS. Cette approche permet de veiller à ce qu'au fil du temps, le Comité ait une compréhension exhaustive des activités du Service. Chaque examen comprend habituellement des conclusions ou des recommandations. Bien que celles-ci ne soient pas de nature contraignante, le SCRS est censé indiquer clairement s'il est d'accord ou non avec les conclusions ou recommandations du CSARS, lesquelles peuvent également amener le Service à modifier ses politiques et procédures internes.

3.49 Le CSARS examine les plaintes dans le cadre d'une audience quasi judiciaire présidée par un membre du Comité avec l'aide du personnel. Les plaintes peuvent être déposées par « toute personne » et peuvent avoir trait aux « activités du Service », comme l'indique la *Loi sur le SCRS*, à la décision d'un autre ministère de refuser une habilitation de sécurité requise ou à des renvois d'Immigration, Réfugiés et Citoyenneté Canada ou de la Commission canadienne des droits de la personne dans les cas d'une plainte relative à la sécurité du Canada. Dans le cadre du processus, le CSARS communique autant de renseignements que possible au plaignant, qui a la possibilité de présenter des observations. Le CSARS présente ensuite des conclusions et des recommandations au gouvernement.

3.50 Les résultats des examens des activités du SCRS par le CSARS sont résumés dans son rapport annuel. Ce rapport est déposé au Parlement, habituellement à l'automne, et il est expurgé afin de protéger la sécurité nationale et la vie privée des intéressés. Le directeur doit également présenter chaque année au ministre un rapport classifié sur les activités opérationnelles du SCRS. Un exemplaire de ce rapport est également remis au CSARS, qui est tenu de certifier au ministre la conformité du SCRS à la *Loi sur le SCRS* et aux instructions ministérielles, y compris si les activités mentionnées dans le rapport comportaient un exercice abusif ou inutile des pouvoirs. Cette fonction complète les évaluations effectuées par le CSARS dans le cadre de ses travaux d'examen.

4.0 Renseignements supplémentaires et rapports

4.1 Pour obtenir de plus amples renseignements sur tout aspect du présent rapport, veuillez communiquer avec Charles Taillefer, directeur, Direction de la politique sur la protection des renseignements personnels et des données, Direction générale des politiques-cadres du marché, Innovation, Sciences et Développement économique Canada, au 235, rue Queen, Ottawa (Ontario) Canada K1A 0H5.

4.2 Il est prévu que les prochains rapports seront présentés à intervalle régulier, soit environ tous les six mois.